CLAIMS

WHAT IS CLAIMED IS:

1. A method, comprising:

reading a media key block from a first region on a medium;

reading validation data related to the media block from a second region on the medium; and

validating the media key block using the validation data.

2. The method of claim 1, wherein said validating the media key block using the validation data comprises:

comparing the media key block (MKB) to the validation data; and

granting authorization to access the content if the media key block corresponds to the validation data.

3. The method of claim 2, wherein the media key block corresponds to the validation data if the media key block matches the validation data.

4. The method of claim 2, wherein the media key block corresponds to the validation data if a hash function over the media key block matches the validation data.

5. The method of claim 4, wherein the validation data comprises a hash function of the media key block, and said validating the media key block comprises:

calculating a first MAC using a message authentication code (MAC) algorithm over the validation data;

calculating a reader hash by using the hash function over the media key block read from the first region of the medium;

calculating a second MAC using the MAC algorithm over the reader hash;

comparing the first MAC to the second MAC; and

verifying the authenticity of the MKB if the first MAC matches the second MAC.

6. The method of claim 1, wherein the medium comprises a DVD-RAM (Digital Versatile Disc - Random Access Memory), and the second region comprises a control data area of the medium.

7. The method of claim 1, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the second region comprises a narrow burst cutting area of the medium.

8. The method of claim 1, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the second region comprises a narrow burst cutting area of the medium.

9. A method, comprising:

on a first device:

reading a first validation data equal to a hash function of the media key block, the validation data being stored in a validation area of the read-only area of a medium; and

calculating a message authentication code (MAC) algorithm over the first validation data to form a first MAC; and

on a second device:

reading a media key block from the medium;

calculating a second validation data equal to the hash function of the media key block read from the medium;

calculating the message authentication code (MAC) algorithm over the second validation data to form a second MAC;

comparing the first MAC and the second MAC; and

verifying the authenticity of the media key block if the first MAC matches the second MAC.

10. The method of claim 9, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the validation area comprises a narrow burst cutting area of the medium.

11. The method of claim 9, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the validation area comprises a narrow burst cutting area of the medium.

12. A method, comprising:

on a first device reading a first validation data equal to a hash function of the media key block, the validation data being stored in a validation area of the read-only area of a medium; and

on a second device:

reading a media key block from the medium;

calculating a second validation data equal to the hash function of the media key block read from the medium;

comparing the first validation data and the second validation data; and

verifying the authenticity of the media key block if the first validation data matches the second validation data.

13. The method of claim 12, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the validation area comprises a narrow burst cutting area of the medium.

14. The method of claim 12, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the validation area comprises a narrow burst cutting area of the medium.

15. A system comprising:

a medium having:

a read-only area;

a writeable area;

a content stored on the writeable area;

a media key block being stored on the medium; and

a first validation data equal to a hash function of the media key block for verifying the authenticity of the media key block, the first validation data being stored in the read-only area;

a drive to:

read the first validation data from the read-only area; and

calculate a message authentication code (MAC) algorithm over the first validation data to form a first MAC; and

a host to:

read a media key block stored on the medium;

calculate a second validation data equal to the hash function of the media key block;

calculate the message authentication code (MAC) algorithm over the second validation data to form a second MAC;

compare the first MAC and the second MAC; and

verify the authenticity of the media key block read if the first MAC matches the second MAC.

16. The system of claim 15, wherein the media comprises one of:

a DVD-R (Digital Versatile Disc - Recordable); and

a DVD-RW (Digital Versatile Disc - Rewriteable).

17. The system of claim 16, wherein the validation area comprises a narrow burst cutting area of the read-only area of the medium.